An Evaluation Ontology Applied to Connected Vehicle Security Assurance

Powley, S., Perry, S., Holt, J. & Bryans, J.

Original citation & hyperlink:
Powley, S, Perry, S, Holt, J & Bryans, J 2019, An Evaluation Ontology Applied to Connected Vehicle Security Assurance. in INCOSE International Symposium: The Proceedings of the Annual INCOSE International Symposium. 1 edn, vol. 29, INCOSE Proceedings, Wiley, USA, pp. 37-52, 29th Annual INCOSE International Symposium, Orlando, United States, 20/07/19.
https://dx.doi.org/10.1002/j.2334-5837.2019.00588.x

DOI 10.1002/j.2334-5837.2019.00588.x
ISSN 2334-5837

Publisher: Wiley

An Evaluation Ontology Applied to Connected Vehicle Security Assurance

Powley, Stephen
Institute for Future Transport and Cities
Priory Street
CV1 5FB
+44 7736 448 738
powleys@uni.coventry.ac.uk

Perry, Simon
Scarecrow Consultants Ltd.

Holt, Jon
Scarecrow Consultants Ltd.

Bryans, Jeremy
Institute for Future Transport and Cities
Priory Street
CV1 5FB
Jeremy.Bryans@coventry.ac.uk

Abstract. Connected vehicles have great potential to benefit society, yet create huge challenges. Vehicles, infrastructure and enterprise activities combine to form massively complex systems of systems (SoSs) that are vulnerable to cyber-attacks. Security is ill-defined, making it difficult to achieve a consistent, common understanding of security capabilities across the diverse industries that collaborate to develop connected vehicles. Rigorous evaluation is essential for developing strong security assurance cases. This paper contributes a model-based systems engineering (MBSE) ontology that enables integrated evaluation processes in enterprise SoSs. The Evaluation Ontology allows diverse types of evaluation to be captured in a single integrated model. A connected vehicle security story is presented to demonstrate the value of the approach. Benefits include enhanced business intelligence that can provide a quantifiable, reportable level of confidence in security-related processes and technologies. Further work will extend the ontology to develop a customisable suite of enabling patterns for security.

Introduction

Modern engineering demands an approach that allows engineers to deal with enormous complexity [Sillito 2014]. Model-based systems engineering (MBSE) has become well established in many industries as a leading means of addressing complexity in security critical systems [Kerzhner et al. 2015] [Oates et al. 2015] [Roudier & Apvrille 2015]. Automotive manufacturers, such as Daimler, have identified MBSE as a means of addressing the multiple strategic challenges that future mobility presents to the industry [Haasis 2016].

Connected vehicles have great potential to benefit society: they can reduce accidents [Yang et al. 2017], reduce pollution [Li, Q 2015] and make journeys quicker and easier. Because they extensively employ networked technologies, they also create great challenges, being massively complex, vulnerable to cyber-attacks, and threatening privacy. To operate securely, connected vehicles must be developed using advanced methods. Organisations often find their existing capabilities to be insufficient.

Connected vehicles and the enterprise environments in which they are created, operated, maintained, retired and destroyed can be considered as complex, software-intensive systems of systems (SoS) [Kurrle, et al. 2016]. This view of connected vehicle enterprises fits with both Maier's criteria [Maier 1998] and Jamshidi's broader definition stating "SoSs are large-scale integrated systems which are heterogeneous and independently operable on their own, but are networked together for a common goal" [Jamshidi 2009].

This paper applies MBSE to systems of systems (SoSs), and addresses the specific problem of how to ensure that evaluation processes across the enterprise are implemented consistently and rigorously. We present an Evaluation Ontology (EO) that provides a basis for a common understanding of evaluation processes across diverse industries, and address the problem of how to ensure that evaluation processes across the enterprise are implemented consistently and rigorously.

EO is one example of a method for enhancing enterprise capability in this regard. By way of example, we apply EO to an automotive security assurance case in consideration of the fact that SoSs "pose particular issues from a security perspective" [INCOSE 2015]. Connectivity brings automotive systems into a realm of previously unheard of complexity and with this comes a pressing need for new methods to assure systems. The complexity also involved in developing secure connected vehicles makes this domain an ideal proving ground for our approach. The EO has much wider applicability to all manner of evaluations, including other types of assurance case.

Enabling ontologies are implementation independent and provide an easily understood way to facilitate the application of MBSE to problems. They can bridge the gap between those responsible for the enterprise system and those responsible for its products and services. By describing required behaviour at a high level they can be specialised and applied to define a coherent set of relevant practices for all activities at all levels of all organisations in an enterprise.

Application to Security

Security is hard to define. Across standards a variety of definitions exist, falling broadly into three categories that identify security as: preserving properties of a system [ISO 2012]; absence of properties from a system [BSI 2018:1085] [BSI 2018:1885]; or a set of measures taken during the lifecycle of the system [Boyes, H and Isbell, R 2017] [BIMCO 2016] [NIST 2014] [SAE 2016]. This represents an additional challenge for those seeking to build secure systems as various stakeholders may have different ideas of what security means, possibly without even realising this. In this work we take the third point of view for consistency with 'SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems' [SAE 2016], which has become established as the leading guideline in the field of automotive cybersecurity.

There is a strong business case for establishing an evaluation framework that can be applied universally across all functions (not just to functions that promote security) within the connected vehicle enterprise. A typical enterprise might comprise a traditional automotive supply chain plus mobility partners, communications networks, app developers, cloud data storage, insurance, recyclers, intelligent transport systems (ITS), emergency services and more. EO spans processes as diverse as: threat/hazard and risk analysis, recruitment, tool selection, sub-system selection, compliance auditing, and design choices, all of which have a bearing on the development of secure systems.

In the remainder of this paper we clarify the Conventions used and present EO. We illustrate a realistic application in An Automotive Security Story and discuss the benefits of the method in the Conclusions. Finally we identify related areas of Further Work.

Conventions

SysML. Diagrams are presented in accordance with 'OMG System Modeling Language' Version 1.3 [Object Management Group 2012] (hereinafter referred to as SysML).

Framework for Architectural Frameworks. The Evaluation Ontology (EO) presented in this paper is constructed in accordance with the SysML-based Framework for Architectural Frameworks (FAF) as described in [Holt, J and Perry, S 2013].

We also adopt the textual notation used in [Holt, J and Perry, S 2013]. Specifically:

- All terms from the SysML notation that form part of the standard are written in italics. Therefore, the use of *block* refers to the SysML construct, whereas the same word without italics – block – refers to an impediment.
- All terms that are defined as part of the overall model presented in [Holt, J and Perry, S 2013] or as part of this paper are presented with capitalised words. Therefore the use of System refers to an Ontology Element called System, whereas the same word without capitals – system – refers to a non-specific usage of the term as a noun or verb. References to section titles in this report are also capitalised.
- All words that are being referenced from a specific diagram are shown in quotes. Therefore, the use of 'Ontology Element' is referring to a specific element in a specific diagram.
- All names are written as singular. Therefore, the term Enabling System may refer to any number of systems, rather than a single one.

Definitions. The following key definitions apply in this document:

enterprise	"one or more organizations sharing a definite mission, goals, and objectives to offer an output such as a product or service" [ISO 2005]
security	measures taken to protect a system against unauthorized access or attack (adapted from the definition of cybersecurity in [SAE 2016])
cybersecurity	"measures taken to protect a cyber-physical system against unauthorized access or attack" [SAE 2016]
evaluation	"making of a judgement about the amount, number, or value of something; assessment" [Oxford 2018]; to apply the Evaluation Ontology to a System

Symbols. Standard SysML symbols are used with the following additions:

Indicates that a block also appears on a separate diagram that describes additional ontology elements and relationships

Thick dashed border indicates the boundary of a Viewpoint. Grey and black are used to assist with distinguishing different boundaries but have no other meaning.

Notes. Please note the following:

- «*ontology element*» appears on most blocks, in several cases the text is truncated with … purely for reasons of space; truncated text has the same meaning as the full term.
- Where the name of an «*ontology element*» contains the symbols :: this indicates that the element is adopted from the patterns described in [Holt, J and Perry, S 2013].

The Evaluation Ontology

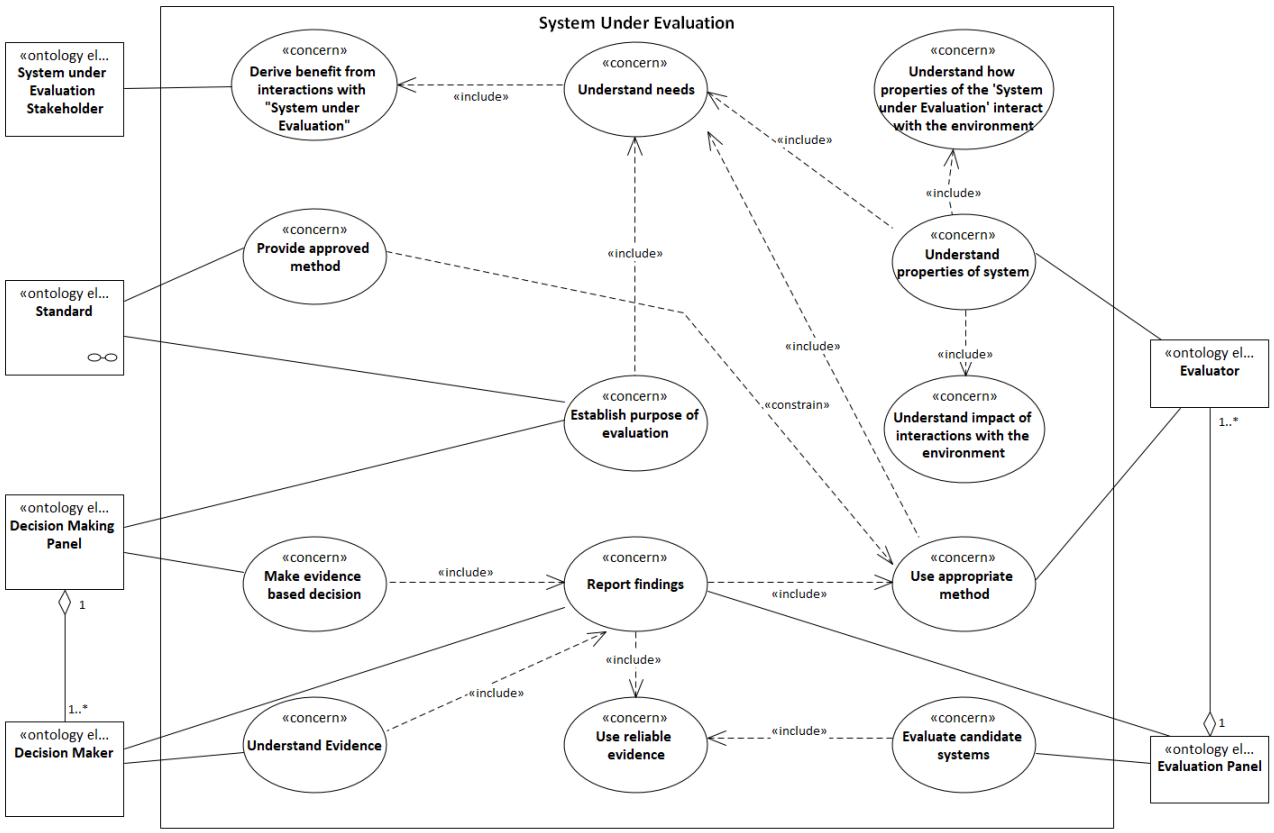

Figure 1: The 'System under Evaluation' context diagram

The Evaluation Ontology (EO), shown in Figure 2, describes a set of concepts and relationships that together facilitate the modelling of evaluation processes and outcomes. The context for the 'System Under Evaluation' is shown in Figure 1. The key actors are represented outside the 'System under Evaluation' boundary as SysML blocks instead of traditional stickmen actors. This approach is recommended by [Weilkiens 2012] for systems of systems. In this work, the intention is to help the reader to visualise the recursive nature in which the ontology should be applied. For example, a person who is an 'Evaluator' in a security assessment would themselves have been the 'System Under Evaluation' when they were going through the recruitment process for their role. This illustrates another important point to bear in mind, which is that this ontology treats human, non-human and mixed groupings as being valid types of System.

The purpose of the ontology is to provide a framework that allows diverse types of evaluation to be captured in a single integrated model. EO can be applied recursively, so models built on EO are flexible and scalable. Every time an evaluation is mapped to the framework, its data becomes available and discoverable across the enterprise in a rigorous, standardised format. The practice of creating a mapping delivers its own benefits as it encourages each 'System under Evaluation Stakeholder' to identify their role(s) and systematically record 'Need', 'Evidence', 'Evaluation Method' and 'Evaluation Result'. This means every mapping of an evaluation is immediately useful, even if not connected to others. So, as is often pragmatic, organisations can start with a small focused study to gain experience with the framework.

To aid with understanding the ontology, we have partitioned it into three viewpoints, as shown by the dashed lines in Figure 2.

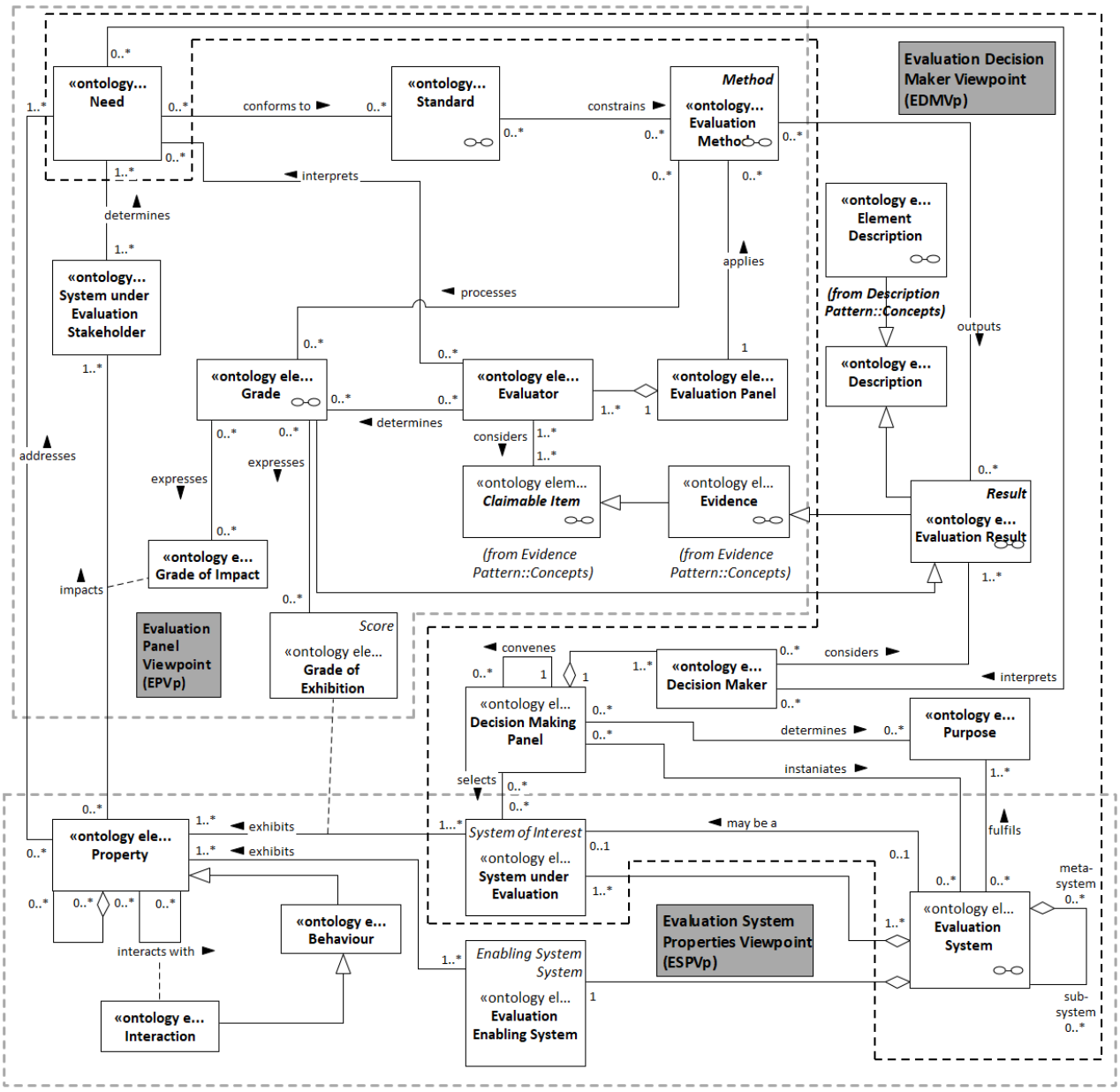

Figure 2. 'Ontology Definition View showing Evaluation Ontology concepts' (additional partitioning to show viewpoints and aid with reading this paper)

The true power of applying the ontology does not manifest until multiple evaluations are captured in an integrated model. Several benefits are summarised in the Conclusions section. To illustrate how a connected vehicle enterprise could benefit from applying EO we have constructed a user story to guide the reader through a realistic application. This is a story we have developed for the purpose of explaining how to apply the Evaluation Ontology in an automotive cybersecurity context. Any resemblance to actual organisations or individuals is coincidental. In future work we intend to conduct a real-world study along similar lines.

A number of design principles were adopted to guide the development of EO:

Maximum applicability. A key purpose of EO is to allow enterprises to capture information about and resulting from all their evaluation processes in a single, integrated model. Therefore it is essential that the ontology is sufficiently generic that it can be applied to any type of evaluation, regardless of

the subject of the evaluations or whether they are performed by human or technical systems (or a combination of the two).

Recursivity. Evaluation systems may themselves be the subject of evaluation, therefore the ontology must be recursive in nature so that it can be applied iteratively.

Consistency. Two of the authors have previously described an extensive and widely implemented ontology for systems engineering [Holt, J and Perry, S 2013]. To maximise the usefulness and ease of implementation of EO, consistency has been maintained with this prior work. This is especially important for future real-world case studies, which we anticipate will take place in organisations already implementing Holt and Perry's ontology. EO is also intended to help organisations improve consistency across their various evaluation processes.

An Automotive Security Story

Chapter 1: Evaluation Decision Maker Viewpoint (EDMVp)

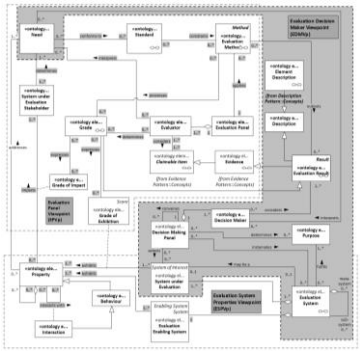

Figure 3: EDMVp scope (included to allow reader to quickly identify EDMVp in Figure 2)

The Scope of the Evaluation Decision Maker Viewpoint is depicted in Figure 3. An automobile manufacturer, Comfortable And Secure Transport (CoAST), develops a security auditing model built on EO. They call this instantiation of 'Evaluation System' the Security Evaluation Approach (SEA) (see Figure 4). Employees at CoAST are working closely with peers in supply chain and partner organisations to develop a new connected vehicle, which they have named CoVe (Connected Vehicle). They are working particularly closely with: Wi-Fi and Audio Vehicle Entertainment (WAVE), who supply a preassembled navigation and communications console, and Big AppY (BAY), who are developing a mobile app that can control vehicle features including door locks. They will conduct a pilot study of SEA across this core group of organisations, which they call the System Architecture Network of Developers (SAND).

Together, CoAST's car platform, WAVE's console and BAY's app form a vehicle System of Systems (SoS). The SAND business processes that must interact in order to develop this vehicle SoS form an enterprise SoS, and the vehicle SoS is an output of the enterprise SoS.

The technical leads for SAND (the SAND leads) at each organisation, Carl, Wendy, and Betty respectively, have formed a 'Decision Making Panel' to steer the development. Carl, Wendy, and Betty 'Need' to ensure that the 'System of Systems' they develop is secure. Their customers 'Need' a usable product. The SAND leads 'Need' to demonstrate that they have taken a structured approach to following the state of the art (in case they ever end up in court). The 'Decision Making Panel' has interpreted these 'Need' to develop the 'Purpose' of SEA. They decide that SEA shall be used to assess and monitor the capabilities of suppliers and partner organisations with respect to the requirements of J3061. They model J3061 as an instance of 'Standard' in SEA. They recognise that there are many other 'Need' relating to the vehicle's security and that implementing J3061 may not

meet them all. It is also clear to them that, for the pilot study, they will not be able to implement the whole guideline. Because they are at the start of their development cycle, they decide to focus on the most relevant guiding principles ('Need') for the pilot study. These are specified in Section 5.4 of J3061 as follows:

5.4 Implement Cybersecurity in Concept and Design Phases

- *Design the feature with Cybersecurity in mind, starting in the concept phase of the development lifecycle. Engineers should consider Cybersecurity when defining the requirements that are to be met for the system and feature(s).*
- *Analyze threats (i.e., initiated external or internal to the system) to determine what will be faced by the system. For the determined threats, identify any vulnerabilities and determine the appropriate Cybersecurity controls.*
- *Implement Cybersecurity analysis (and management tools) that enable engineers to determine and configure the optimal Cybersecurity level for the system.*

Interpreting these 'Need' leads the 'Decision Making Panel' to identify that several interrelated evaluations will be required. They decide to decompose the SEA 'Evaluation System' into three child systems, each of which is an 'Evaluation System' in its own right. The purposes of the evaluations are therefore:

1. Establish capability of organisations to "Design the feature with Cybersecurity in mind"
2. "Analyze threats … to determine what will be faced by the system"
3. Choose "cybersecurity analysis techniques and management tools"

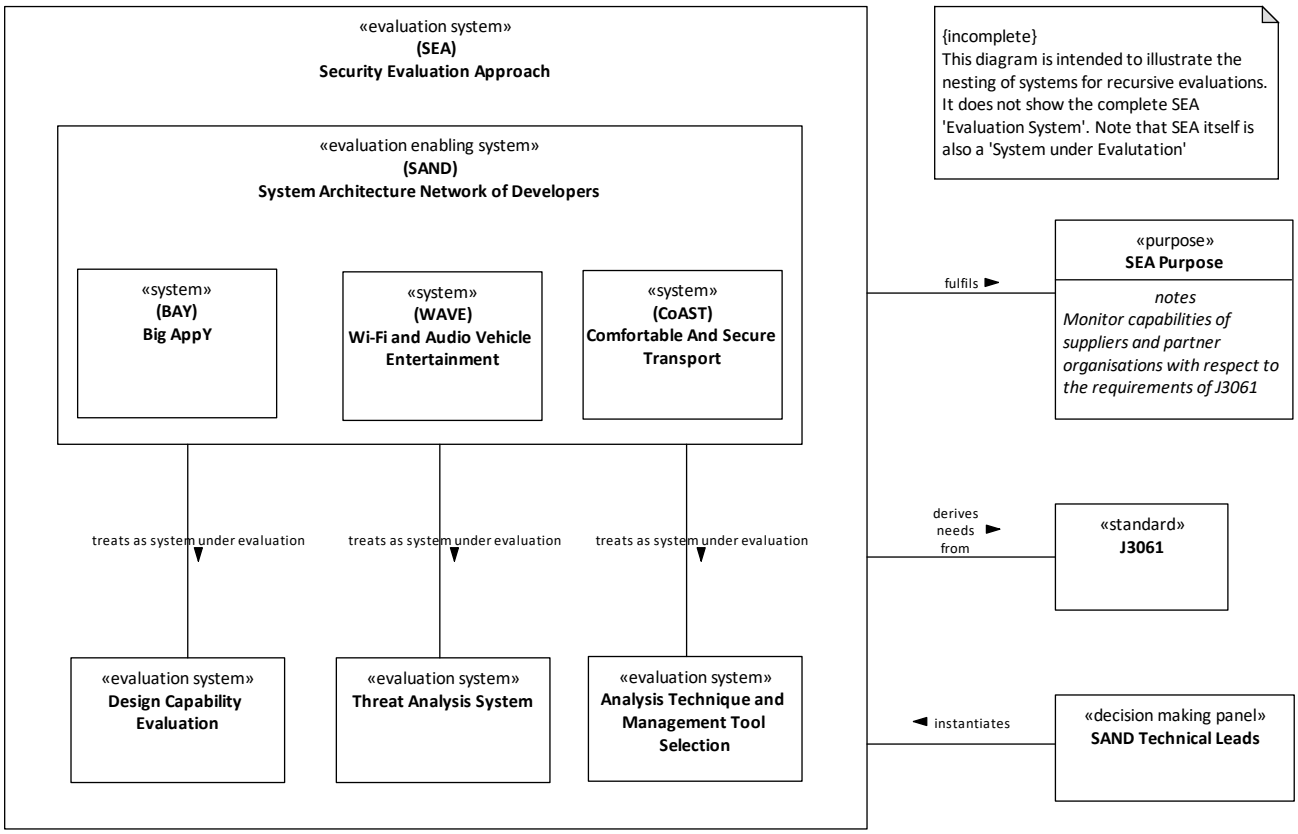

Figure 4: Nested evaluations in the Security Evaluation Approach

Chapter 2: Evaluation System Properties Viewpoint (ESPVp)

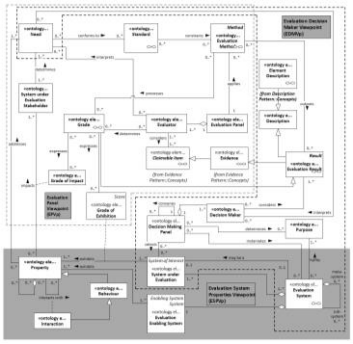

Figure 5: ESPVp scope (included to allow reader to quickly identify ESPVp in Figure 2)

Having decided on the ‘Purpose’ for their four ‘Evaluation System’ (one parent system with three child systems), the SAND leads can now set up (instantiate) those systems. Figure 6 illustrates how the various concepts related to ‘System’ are structured.

The ‘Evaluation System’ will be run by humans (as is normally the case at present). The key task is to appoint the ‘Evaluation Panel’ for the parent and child evaluations (4 panels). One person from each SAND organization is nominated to each panel, with CoAST chairing (as the major stakeholder). The SAND leads do not include themselves, instead choosing to be part of the parent evaluation that will roll up the results. They decide that the parent evaluation should also include representatives from each of the child evaluations, with Carl as chair. They also agree and document the terms of reference for the panels. Finally, they agree that the ‘Decision Making Panel’ that considers the ‘Evaluation result’ of the parent evaluation will comprise the SAND leads plus one of CoAST’s chief engineers. They agree that decisions will be made by majority vote, with the chief engineer having final authority in the case of a split decision. Note that the child evaluations do not include a ‘Decision Making Panel’ because they are leaves in the ‘Evaluation System’ SoS model. Correspondingly, the highest level in the model is the original ‘Decision Making Panel’, which exists as an external actor outside the parent ‘Evaluation System’. Of course, the members of the ‘Decision Making Panel’ were themselves the subjects of an evaluation in order to gain their roles, but SAND has not (yet) captured that in the model.

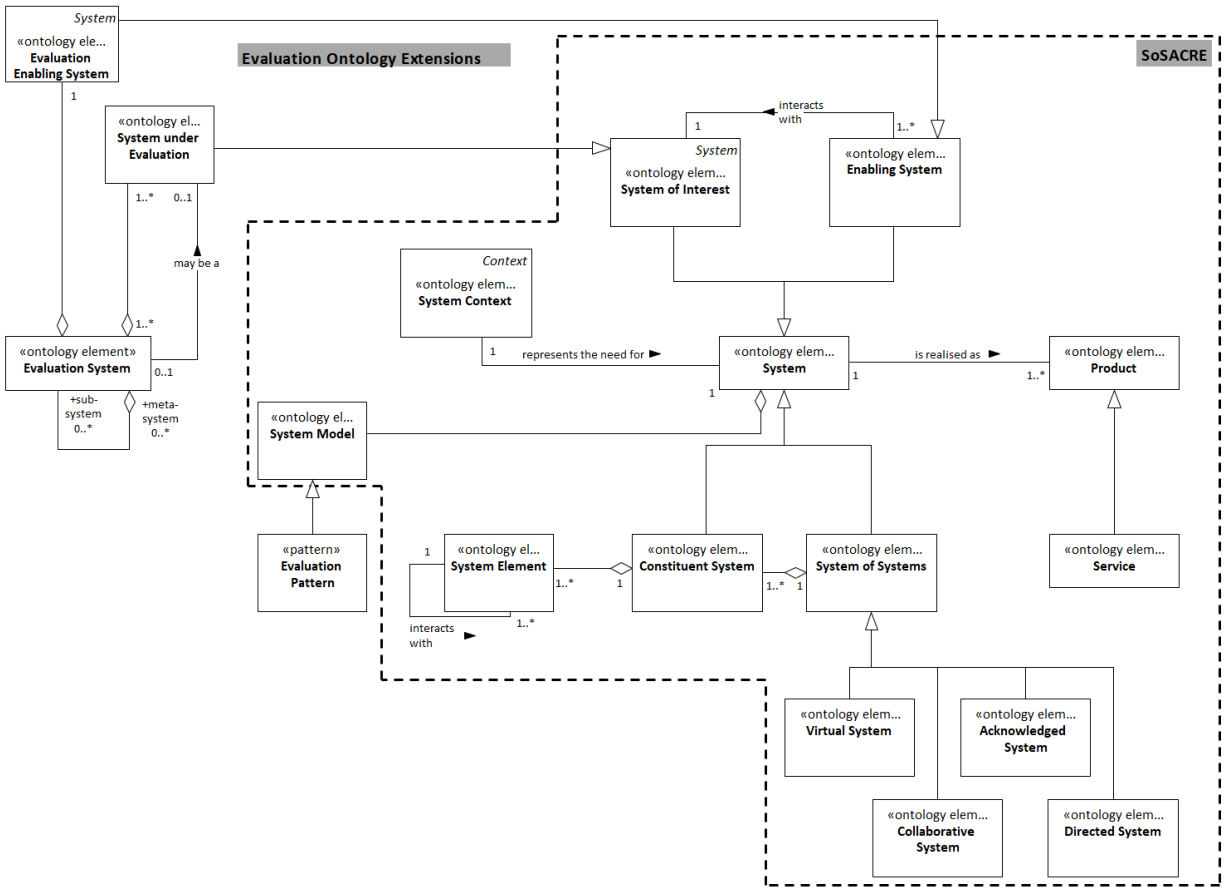

Figure 6: Evaluation System Concepts extending SoSACRE [Holt, J and Perry, S 2013]

The ‘Decision Making Panel’ must now select one or more candidates for the ‘System Under Evaluation’ in each ‘Evaluation System’, taking into account the ‘Property’ that are relevant to the ‘Purpose’. Note that the concept of ‘Property’ includes ‘Behaviour’:

1. Establish capability of organisations to “Design the feature with Cybersecurity in mind”:
   Conduct an audit whereby the ‘System Under Evaluation’ are the employees in SAND responsible for (a) defining the requirements that are to be met by the system and feature(s) and (b) designing the features. The ‘Property’ of interest will be employees’ knowledge, skills and experience relating to cybersecurity-by-design.
2. “Analyze threats … to determine what will be faced by the system”:
   Conduct a Threat and Risk Assessment (TARA) whereby the ‘System Under Evaluation’ is CoVe and the environment in which it operates. The ‘Property’ of interest will be the threats that CoVe is exposed to when operating.
3. Choose “cybersecurity analysis (and management tools)”
   Perform a trade-off study whereby the ‘System Under Evaluation’ is multiple vulnerability databases that could be used to assist with cybersecurity analysis. The SAND leads note that there are many other analysis and management tools and techniques that they need to understand better, however they need to constrain the scope of the pilot study. They have noticed that the different organisations in SAND all use different databases currently, so understanding their relative merits will be a useful place to start. They instruct the ‘Evaluation Panel’ to survey users about the important features (the ‘Property’) of the database they use already, what features they would like to have, and then to compare how well each of the candidate databases meets users’ ‘Need’ through its implementation of the required features.

Recall that the purpose of SEA is to "assess and monitor the capabilities of suppliers and partner organisations with respect to the requirements of J3061". The SEA 'Evaluation system' (parent) will consider each of the three child evaluations as a 'System Under Evaluation' and each of their 'Evaluation Result' will serve as evidence. Because CoAST's own activities have been included in the pilot study, this means that CoAST will be able to compare their suppliers' capability against their own as a benchmark. The main 'Property' of interest for each child 'System Under Evaluation' is its ability to generate evidence that helps with assessing and monitoring capabilities with respect to J3061.

Chapter 3: Evaluation Panel Viewpoint (EPVp)

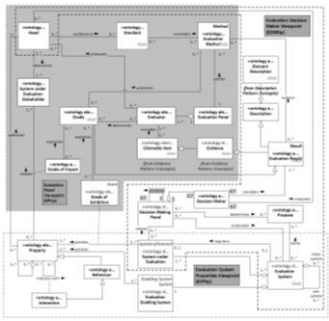

Figure 7: EPVp scope (included to allow reader to quickly identify EPVp in Figure 2)

The SAND leads ask each 'Evaluation Panel' to ensure it has understood its remit and allocate elements of the evaluation to different 'Evaluator'. Some 'Grade' may be determined by more than one evaluator to gain different perspectives, especially if there is subjectivity or risk of error involved. It may also not be possible to determine 'Grade' for every 'Property', for example if suitable measurement equipment is not available.

'Evaluator' interprets the set of 'Need' of each 'System of Interest Stakeholder' to make sure that every property that has a relevant impact is considered. They then establish the 'Grade of Exhibition' to establish the quality with which 'System Under Evaluation' exhibits each 'Property'. In engineering, 'Grade of Exhibition' will typically be a 'Quantity Value' (e.g. current rating of a wire) or a more subjective expression of how well a property is exhibited (e.g. high voltage). Figure 8 shows an example of how different types of 'Grade' might be organised. Next, an 'Evaluator' (often, but not necessarily, the same person) revisits each 'Property' to assign a 'Grade' that describes its impact on the affected 'System Under Evaluation stakeholder'.

'Evaluator' considers one or more 'Claimable Item' to assist them in determining 'Grade'. Typically this would be some pieces of hard 'Evidence', such as measurements, but could also be an unsubstantiated claim. For example, a vendor might claim that they use a certain strength of encryption, but SAND does not have the capability to verify this. Once all 'Grade' have been assigned, the 'Evaluation Panel' can apply a 'Method' to make sense of the collected 'Grade'. In the simplest case this may simply be to pass all 'Grade' to a 'Decision Maker', but it could involve using a computed 'Algorithm' or following a written procedure.

SAND applies the following 'Method':

1. A comparison of all key staff competences related to security-by-design against a security skills matrix developed specifically for the purpose.
2. A Threat and Risk Analysis (TARA) using the E-Safety Vehicle Intrusion Protected Applications (EVITA) method from J3061. J3061 also recommends other methods, so the 'Evaluation Panel' includes a recommendation in its report (the 'Evaluation Result') that a separate evaluation of TARA methods should be performed to determine the one that best fits their 'Need'. This best-fit

study is outside the scope of the pilot, so they choose EVITA because they all enjoyed the musical! (This illustrates the serious point that not all decisions are taken on the basis of hard facts.) Even if the 'Evaluation Panel' do not record their questionable reasoning, an appropriate query on the model will still reveal that the decision was not underpinned by an item of 'Evidence'. This might even serve as the trigger for another evaluation to establish a more suitable decision making process!

3. 'Evaluation Panel' performs the 'Need' survey across the different organisations and applies a method that rolls up the 'Grade' to give a set of 'Score' that describe the relative strengths of the databases already in use alongside alternative options.

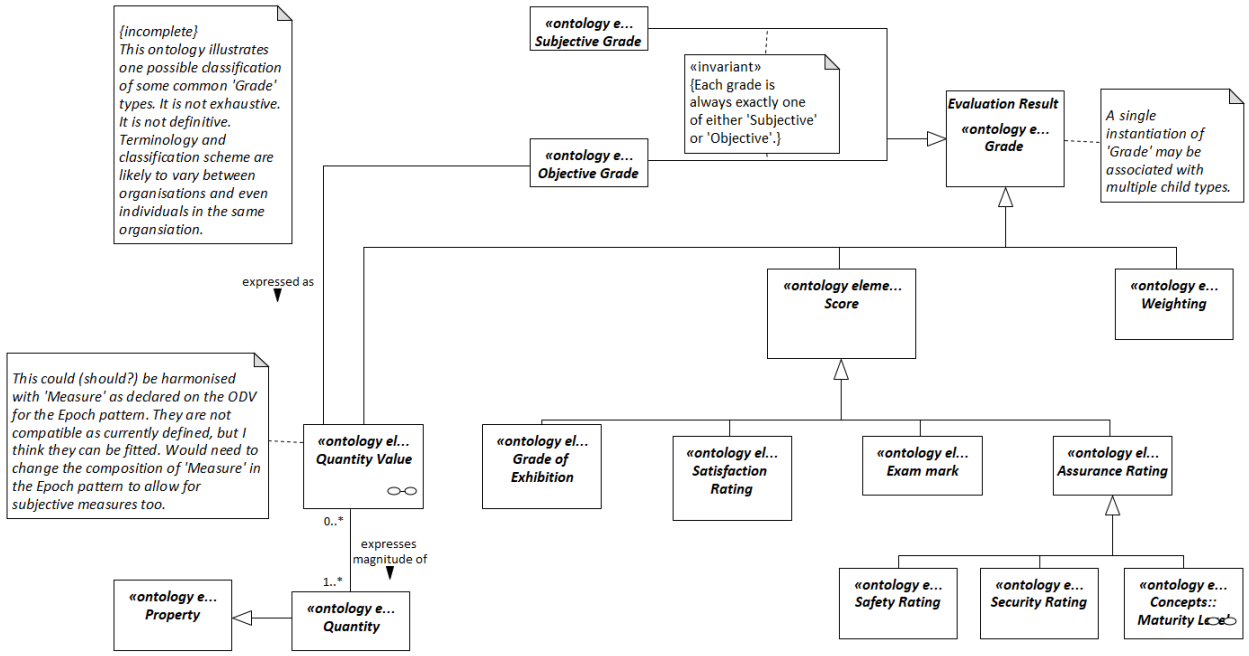

Figure 8: Ontology of 'Grade' types

Finally, the SEA 'Evaluation Panel' assigns a set of 'Grade' that express the effectiveness of the three child evaluations with respect to their ability to "assess and monitor the capabilities of suppliers and partner organisations with respect to the requirements of J3061". This requires a much more subjective method because, in this first instance, no benchmarks exist against which to compare the outputs of the child evaluations. They are careful to record their assumptions in their report so that these can be scrutinised when SEA is repeated and the organisations have more experience. The 'Evaluation Panel' also reports on how SEA might be strengthened after the pilot study by adding further aspects of J3061 and other 'Standard' to the evaluation mix.

Conclusions

The Evaluation Ontology is a flexible, robust basis for modelling evaluation processes throughout an enterprise. It allows results from diverse evaluation practices to be mapped to a common pattern without requiring changes to existing processes. In An Automotive Security Story we have shown how to begin applying the Evaluation Ontology (EO) recursively to develop an evaluation tree that has both breadth and depth in terms of its reach in the enterprise. This makes it a scalable approach that delivers both immediate and long-term gains. We have identified a number of benefits of applying EO and cross reference these to the examples in the user story. The benefits are:

- A common description of the way evaluation processes are implemented across the enterprise.
    - SAND was able to model the processes of three different organisations to assess capability with respect to J3061.
- A means of combining disparate evaluation types (subjective and objective) to allow roll-up of results. Applicable to both technical (e.g. security hardware/software) and human aspects of systems (e.g. recruitment, user experience, review panel).
    - SAND decomposed its capability assessment to apply the ontology to evaluating human security skills, performing a TARA, and comparing security databases.
- Tailoring the granularity of the model to match the level of rigour expected in evaluations of all types.
    - In their reports, the 'Evaluation Panel' were careful to identify further evaluations that would benefit the company. Without the awareness of the connectedness that applying the ontology brings, they would have been less likely to include this aspect in their reports.
- Querying the model for business intelligence to identify areas of good and poor practice.
    - The same evaluations performed in isolation would have delivered insights into three different business areas, but the relationships between them would not have been captured. The querying power of the model grows exponentially as more evaluations are mapped, but even a small sample will raise awareness of, for example, how a recruitment process can impact a comparison of databases.
- Straightforward gap analysis between required capabilities (e.g. as per J3061 [SAE 2016] and other emerging standards) and existing capabilities.
    - Even with a small pilot, the simple fact of the rigour imposed on SAND by the ontology meant the partner organisations quickly gained a clear impression of how much J3061 demanded, how far they had to go, and how they could support each other.
- Gaining a quantifiable, reportable level of confidence in security-related evaluations in all business areas e.g. for decision making, auditing.
    - Simply applying EO is enough to bring rigour to recording and reporting processes. Discoverability of information for business intelligence is greatly enhanced by applying EO. The company also gains by having documentation to prove they followed a structured process.
- Quantifying the impact of decision making processes on the quality of upstream/downstream evaluations.
    - SAND now has an additional capability from the pilot that allows them, for example, to map the impact of employee skills in a supplier organisation to the security of the buyers' products.

The example considered in this work focuses on evaluation activities performed in early lifecycle stages. It should be noted that evaluation processes are key to successful engineering outcomes at all stages of the product and service lifecycle – verification and validation activities, for example, are by their very nature types of evaluation. EO has be structured so that it can be applied at any and all lifecycle stages. Applying the ontology widely across an enterprise provides valuable traceability between multiple evaluations and evaluation results, which can be leveraged extensively to provide intelligence about the quality of business and engineering processes and the products and services they deliver.

Further Work

Our goal is to develop a set of enabling patterns that can be applied to deliver acceptable and agreed levels of security throughout the connected vehicle lifecycle. To this end we will continue to develop new enabling patterns and extend those presented in [Holt, J and Perry, S 2013] and its companion volume [Holt et al. 2016]. The next step is to develop the Evaluation Ontology into a full Enabling

Pattern with Viewpoints, Views and rule sets. We will also develop specialisations of the Evaluation Pattern to address specific types of evaluation (e.g. TARA, HARA, recruitment, tool selection). We anticipate then creating a corresponding SysML profile and exploring a real-world implementation with automotive partners.

In this paper we have considered a process-centric view of security as followed in J3061. However, to be able to service all interpretations of security we will develop additional patterns that can be combined as customised security meta-patterns to deliver the specific security properties required in each unique system. The properties we target initially will be those identified in the classic CIA[1] (confidentiality, integrity and availability) triad of information security. Further, we will consider the additional properties proposed in the Information Assurance & Security (IAS) Octave [Schmidt, K et al. 2014] (privacy, authenticity & trustworthiness, non-repudiation, accountability, and auditability) and in the HEAVENS project [Lautenbach, A et al. 2016] (authenticity, authorization, non-repudiation, privacy, and freshness).

We have identified two key patterns for immediate attention that we expect to help deliver the required properties. Evolvability is essential because the security threat landscape is in constant flux. Measurement, closely related to evaluation, is a natural candidate to complement the Evaluation Pattern.

To ensure that our patterns meet real needs, we have planned a series of structured interviews with representative stakeholders from a wide range of industries involved in connected vehicles. We are also actively seeking organisations to provide real-world case studies that demonstrate the value of EO and future patterns applied in practice. The corresponding authors would welcome enquiries from interested organisations.

EO accommodates both qualitative and quantitative evaluation methods and provides the basis for combining the two into a common framework. When EO is applied in practice, it will be essential to understand what can be measured in order to evaluate the effectiveness of applying EO. Where possible and relevant, key performance indicators used to describe the quality of existing evaluation processes will be adopted so organisations have a baseline against which to measure improvement. However, we anticipate that in many cases relevant indicators will not be actively measured with current practice. In the absence of such baseline indicators we will seek to demonstrate the following: value of traceability where none previously existed; facilitation of process consistency and reusability; new ability to align processes (within organisations and across supply chains and collaboration partners) and perform impact analysis; that EO is applicable to many types of evaluations. If possible, we would also apply EO retrospectively to a completed project that did not apply EO originally in order to establish what benefits might have been seen had it been used.

Finally, because of the important relationship between security and safety, we also intend to clearly define relevant interfaces. We hope to demonstrate that many of the enabling patterns that benefit security will also work to the benefit of safety and other desirable system properties.

Acknowledgement

The authors acknowledge the valuable contribution of James Towers, Object Flow Ltd., who provided a careful and insightful review of this paper.

[1] The exact origins of the CIA triad appear to be unknown. The underlying concepts have been applied in military circles at least since Roman times [Pornin 2013]

References

BIMCO 2016, 'The Guidelines on Cyber Security onboard Ships', BIMCO, (Bagsvaerd DK)

Boyes, H and Isbell, R 2017, 'Code of Practice: Cyber Security For Ships', The Institution of Engineering and Technology (London UK)

British Standards Institution 2018, 'PAS 1085:2018. Manufacturing – Establishing and implementing a security-minded approach – Specification', BSI Standards Ltd. (London UK)

British Standards Institution 2018, 'PAS 1885: 2018 - The fundamental principles of automotive cyber security - Specification', BSI Standards Ltd. (London UK)

Holt, J and Perry, S 2013, *SysML for Systems Engineering: 2nd Edition: A model-based approach*, The Institution of Engineering and Technology (London UK)

Holt, J et al. 2016, *Foundations for Model-based Systems Engineering: From Patterns to Models*, The Institution of Engineering and Technology (London UK)

Haasis, S 2016 'Systems Engineering for Future Mobility' REConf®, viewed 16 November 2018, https://www.hood-group.com/fileadmin/projects/hood-group/upload/Images/REConf/2016/vortraege/mittwoch/auditorium/Keynote-Systems_Engineering_for_future_mobility.pdf (Stuttgart DE)

International Organization for Standardization 2005, 'Industrial automation systems – Requirements for enterprise-reference architectures and methodologies. ISO 15704:2000 incorporating ISO amendment 1:2005', International Organization for Standardization, (Geneva CH)

International Organization for Standardization, International Electrotechnical Commission 2012, 'ISO/IEC 27032:2012 – Information technology — Security techniques — Guidelines for cybersecurity', BSI Standards Ltd. (London UK)

International Council on Systems Engineering 2015, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities Fourth Edition*, International Council on Systems Engineering, (San Diego US)

Jamshidi, M ed, 2009, *Systems of Systems Engineering: Principles and Applications*, CRC Press (Boca Raton US)

Kerzhner, A et al. 2015, 'Analyzing Cyber Security Threats on Cyber-Physical Systems using Model-Based Systems Engineering', AIAA SPACE Conference and Exhibition 2015, Jet Propulsion Laboratory, National Aeronautics and Space Administration, (Pasadena, US)

Kurrle, A, Albers, A and Klinger, S 2016, 'The Connected Car – A system-of-systems: Exploration of challenges in development from experts view', Wiesbaden, Springer Fachmedien (Wiesbaden DE)

Lautenbach, A, Islam, M 2016, 'HEAVENS – HEAling Vulnerabilities to ENhance Software Security and Safety', The HEAVENS Consortium (Borås SE)

Li, Qing, Qiao, F and Yu, L 2015, 'Will Vehicle and Roadside Communications Reduce Emitted Air Pollution?', International Journal of Science and Technology, Volume 5 No.1, IJST Publications (UK)Mari, L and Giordani, A 2012, 'Quantity and quantity value', Metrologia, Volume 49, Number 6, BIPM & IOP Publishing Ltd. (Bristol UK)

Maier, M 1998, 'Architecting Principles for System of Systems', *Systems Engineering*, Volume 1, International Council on Systems Engineering, (San Diego US)

National Institute of Standards and Technology (NIST) 2014, 'Framework for Improving Critical Infrastructure Cybersecurity', National Institute of Standards and Technology (NIST) (Gaithersburg US)

Oates, R, Thom, F and Herries, G 2015, 'Security-Aware, Model-Based Systems Engineering with SysML', in Janicke, H and Jones, K (ed.) 'Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, '1st International Symposium for ICS & SCADA Cyber Security Research', British Computer Society Learning and Development Ltd. (Leicester UK)

Object Management Group 2012, 'Omg System Modeling Language Specification Version 1.3', Object Management Group, viewed 15 March 2019, <https://www.omg.org/spec/SysML/1.3/>

Oxford Dictionaries 2018, 'Oxford English Dictionary', Oxford University Press, viewed 14 November 2018, <https://en.oxforddictionaries.com/definition/evaluation>

Pornin , T 2013, StackExchange, Information Security, viewed 16 November 2018, <https://security.stackexchange.com/questions/47697/who-is-the-creator-of-the-cia-triad>

Roudier, Y and Apvrille, L 2015, 'SysML-Sec: A model driven approach for designing safe and secure systems', 3rd International Conference on Model-Driven Engineering and Software Development, MODELSWARD.

SAE International 2016, 'Cybersecurity Guidebook for Cyber-Physical Vehicle Systems: J3061', SAE International (Warrendale US)Schmidt, K, Tröger, P, Kroll, H, Bünger, T. et al. 2014, 'Adapted Development Process for Security in Networked Automotive Systems', SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 7(2):2014

Sillitto, H 2014, *Architecting Systems - Concepts, Principles and Practice*, College Publications

Weilkiens, T 2012, 'The Death of the Actor', MBSE4U, viewed 15 November 2018, <https://model-based-systems-engineering.com/2012/03/20/the-death-of-the-actor/>

Yang, H, Wang, Z and Xie, K 2017, 'Impact of connected vehicles on mitigating secondary crash risk', *International Journal of Transportation Science and Technology*, Volume 6, Issue 3, Tongji University Press (Tongji CN)

Biography

Stephen Powley MEng MINCOSE MIET. Stephen's vision is for a harmonious, interconnected world that understands how to use technology to break down barriers and bridge divides. Before starting his PhD in Automotive Cybersecurity, he consulted on requirements-led engineering for international businesses. His research focuses on describing how enterprises with global impact can work together to deliver complex, high-integrity automotive systems that remain secure throughout their lifecycles.

Stephen works actively as a volunteer sharing the wonder of engineering and technology with young people. He co-founded Robot Day in Derby and Coventry, UK – the most recent event attracted over 5500 visitors of all ages.

Simon Perry BSc PGC IS MINCOSE MIET. Simon holds Bachelor of Science degrees from both the University of Leeds and the Open University. Since gaining his Mathematics degree in 1986 he has spent over 30 years working in all aspects of software and systems engineering. Since 2014 he has been a Director and consultant for Scarecrow Consultants. He often speaks at systems engineering conferences and is the author of 10 books on systems engineering and related topics. Such public-speaking events, book writing and the delivery and facilitation of courses and workshops, have given Simon great experience in communicating technical concepts to non-domain experts and non-technical audiences.

Dr. Jeremy Bryans MINCOSE. Jeremy is an Assistant Professor in Automotive Cybersecurity at Coventry University, seeking to answer the questions: how can we build secure systems, and how can we demonstrate that they are secure? He has substantial experience in developing and applying formal verification methods and techniques to problems of security, dependability and resilience within large systems including socio-technical systems, systems of systems and cyber-physical systems.

Prof. Jon Holt CEng CITP FIET FBCS MINCOSE. Jon is an internationally-recognised expert in the field of Model-based Systems Engineering (MBSE), an international award-winning author and public speaker and has authored 15 books on MBSE and its applications. He is a director and consultant for Scarecrow Consultants and Professor of Systems Engineering at Cranfield University. He is Technical Director of INCOSE UK and, in 2015, was identified as one of the 25 most-influential Systems Engineers in the last 25 years by INCOSE.

Jon actively promotes Science, Technology, Engineering and Mathematics (STEM) using magic, mind-reading and escapology to promote Systems Engineering. He authored the children's STEM book 'Think Engineer'.